THAT WHICH IS CLAIMED:

1. A method of controlling access to digital data in a file comprising:

obtaining a passphrase from a user;

generating a personal key based on the obtained passphrase;

generating a file encryption key;

encrypting the digital data in the file with the file encryption key to provide an encrypted file;

encrypting the file encryption key with the personal key to provide an encrypted file encryption key;

creating a file header containing the encrypted file encryption key; and

associating the file header with the encrypted file.

2. A method according to Claim 1, further comprising the step of storing the encrypted file at a file server.

3. A method according to Claim 2, wherein the passphrase comprises a current passphrase and wherein the step of storing the encrypted file is followed by the steps of:

obtaining the file header associated with the encrypted file stored at the file server;

generating the personal key from the current passphrase associated with the file;

decrypting the encrypted file encryption key with the personal key to provide a recovered file encryption key;

generating a new personal key based on a new passphrase;

encrypting the file encryption key with the new personal key to provide a new encrypted file encryption key;

creating a new file header containing the new encrypted file encryption key; and

associating the new file header with the encrypted file stored at the file server.

4. A method according to Claim 3, further comprising the step of storing the new file header associated with the encrypted file at the file server.

5. A method according to Claim 4, wherein a plurality of files have corresponding associated file headers containing encrypted file encryption keys encrypted with a corresponding plurality of personal keys based on the passphrase, and wherein the step of obtaining the file header associated with the encrypted file comprises the step of retrieving the plurality of file headers associated with the encrypted files from the file server;

wherein the step of generating the personal key from the current passphrase associated with the file comprises the step of generating the plurality of personal keys from the current passphrase associated with the plurality of files;

wherein the step of decrypting the encrypted file encryption key with the personal key to provide a recovered file encryption key comprises the step of decrypting the plurality of encrypted file encryption keys with corresponding ones of the plurality of personal keys to provide a corresponding plurality of file encryption keys;

wherein the step of generating a new personal key based on the new passphrase comprises the step of

generating a plurality of new personal keys based on the new passphrase;

wherein the step of encrypting the file encryption key with the new personal key to provide a new encrypted file encryption key comprises the step of encrypting the plurality of file encryption keys with corresponding ones of the plurality of new personal keys to provide a plurality of new encrypted file encryption keys;

wherein the step of creating a new file header containing the new encrypted file encryption key comprises the step of creating a plurality of new file headers containing the new encrypted file encryption keys; and

wherein the step of storing the new file header associated with the file at the file server comprises the step of storing the plurality of new file headers associated with the plurality of files at the file server.

6. A method according to Claim 5, wherein the plurality of files comprise all files stored at the file server associated with a user and having a file header with an encrypted file encryption key encrypted with a personal key derived from the current passphrase.

7. A method according to Claim 2, wherein the step of storing the encrypted file is followed by the steps of:

obtaining a passphrase to be utilized in decrypting the file;

retrieving the encrypted file and the associated file header;

generating the personal key from the passphrase to be utilized in decrypting the file;

decrypting the encrypted file encryption key with the personal key to provide a recovered file encryption key; and

decrypting the file with the recovered file encryption key.

8. A method according to Claim 1, further comprising the steps of:

obtaining a user identification associated with an owner of the file;

obtaining a file identification associated with the file; and

wherein the step of generating a personal key based on the obtained passphrase comprises the step of hashing the user identification, the passphrase and the file identification to provide the personal key.

9. A method according to Claim 8, further comprising the step of storing the file and the associated file header at a file server.

10. A method according to Claim 9, wherein the step of storing the file and the associated file header at a file server comprises the step of selectively storing the file and the file header based on a type of store requested by the user and an evaluation of whether an existing file and file header having the user identification and file identification are stored at the file server.

11. A method according to Claim 1, further comprising the steps of:

generating an integrity key;

generating a message authentication code based on digital data of the file utilizing the integrity key;

wherein the step of encrypting the file encryption key with the personal key to provide an encrypted file encryption key comprises the step of encrypting the file encryption key and the integrity key with the personal key to provide encrypted file encryption keys; and

wherein the step of creating a file header containing the encrypted file encryption key comprises the step of creating a file header containing the encrypted file encryption keys and the message authentication code.

12. A method according to Claim 11, further comprising the step of storing the encrypted file and the file header associated with the encrypted file at a file server.

13. A method according to Claim 12, wherein the step of storing the encrypted file and the file header is followed by the steps of:

obtaining a passphrase to be utilized in decrypting the file;

retrieving the encrypted file and the associated file header from the file server;

generating the personal key from the passphrase to be utilized in decrypting the file;

decrypting the encrypted file encryption keys with the personal key to provide a recovered file encryption key and a recovered integrity key;

decrypting the file with the recovered file encryption key;

hashing the recovered integrity key with the decrypted file to provide a recovered message authentication code;

obtaining the message authentication code from the file header; and

comparing the recovered message authentication code with the message authentication code from the file header to confirm that the decrypted file corresponds to the file which generated the message authentication code from the file header.

14. A method according to Claim 11, further comprising the step of hashing the file encryption key with the integrity key to provide a verification value; and

wherein the step of encrypting the file encryption key and the integrity key with the personal key to provide encrypted file encryption keys comprises the step of encrypting the file encryption key, the integrity key and the verification value with the personal key to provide the encrypted file encryption keys.

15. A method according to Claim 14, further comprising the step of storing the encrypted file and the file header associated with the encrypted file at a file server.

16. A method according to Claim 15, wherein the step of storing the encrypted file and the file header is followed by the steps of:

obtaining a passphrase to be utilized in decrypting the file;

retrieving the encrypted file and the associated file header from the file server;

generating the personal key from the passphrase to be utilized in decrypting the file;

decrypting the encrypted file encryption key with the personal key to provide a recovered file encryption key, a recovered integrity key and a recovered verification value;

hashing the recovered file encryption key and the recovered integrity key to provide a hash value;

comparing the hash value and the recovered verification value; and

decrypting the file with the recovered file encryption key if the comparison of the hash value and the recovered verification value indicates that the values are equal.

17. A method according to Claim 16, further comprising the steps of:

hashing the recovered integrity key with the decrypted file to provide a recovered message authentication code;

obtaining the message authentication code from the file header; and

comparing the recovered message authentication code with the message authentication code from the file header to confirm that the decrypted file corresponds to the file which generated the message authentication code from the file header.

18. A method according to Claim 1, further comprising the steps of:

determining if a party other than an owner of the file is to have access to the file;

obtaining a public key associated with the party other than the owner of the file if the party other

than the owner of the file is to have access to the file;

encrypting the file encryption key with the public key of the party other than the owner of the file to provide a public key encrypted file encryption key if the party other than the owner of the file is to have access to the file; and

incorporating the public key encrypted file encryption key in the header associated with the file if the party other than the owner of the file is to have access to the file.

19. A method according to Claim 18, further comprising the step of storing the file header and the file at a file server.

20. A method according to Claim 19, wherein the step of storing the file header and the file at the server is followed by the steps of:

retrieving the file and the file header from the file server;

obtaining a private key associated with the public key;

decrypting the public key encrypted file encryption key with the private key to provide the file encryption key; and

decrypting the file with the file encryption key.

21. A method according to Claim 18, further comprising the steps of:

generating an integrity key;

generating a message authentication code based on digital data of the file utilizing the integrity key;

wherein the step of encrypting the file encryption key with the personal key to provide an encrypted file

encryption key comprises the step of encrypting the file encryption key and the integrity key with the personal key to provide encrypted file encryption keys;

wherein the step of creating a file header containing the encrypted file encryption key comprises the step of creating a file header containing the encrypted file encryption keys and the message authentication code;

wherein the step of encrypting the file encryption key with the public key of the party other than the owner of the file to provide a public key encrypted file encryption key if the party other than the owner of the file is to have access to the file comprises the step of encrypting the file encryption key and the integrity key with the public key to provide public key encrypted keys; and

wherein the step of incorporating the public key encrypted file encryption key in the file header associated with the file if the party other than the owner of the file is to have access to the file comprises the step of incorporating the public key encrypted keys in the file header.

22. A method according to Claim 21, further comprising the step of storing the encrypted file and the file header associated with the encrypted file at a file server.

23. A method according to Claim 22, wherein the step of storing the encrypted file and the file header is followed by the steps of:

retrieving the encrypted file and the associated file header from the file server;

obtaining a private key associated with public key;

decrypting the public key encrypted keys with the private key to provide a recovered file encryption key and a recovered integrity key;

decrypting the file with the recovered file encryption key;

hashing the recovered integrity key with the decrypted file to provide a recovered message authentication code;

obtaining a message authentication code from the file header; and

comparing the recovered message authentication code with the message authentication code from the file header to confirm that the decrypted file corresponds to the file which generated the message authentication code from the file header.

24. A method according to Claim 22, wherein the public key comprises a current public key and wherein the step of storing the encrypted file and the file header is followed by the steps of:

retrieving the file header associated with the encrypted file from the file server;

generating the personal key from the passphrase associated with the file;

decrypting the encrypted file encryption key with the personal key to provide a recovered file encryption key;

obtaining a new public key;

encrypting the file encryption key with the new public key to provide a new public key encrypted file encryption key;

creating a new file header containing the new public key encrypted file encryption key; and

storing the new file header associated with the file at the file server.

25. A method according to Claim 21, further comprising the step of hashing the file encryption key with the integrity key to provide a verification value; and

wherein the step of encrypting the file encryption key and the integrity key with the public key to provide public key encrypted keys comprises the step of encrypting the file encryption key, the integrity key and the verification value with the public key to provide the public key encrypted keys.

26. A method according to Claim 25, further comprising the step of storing the encrypted file and the file header associated with the encrypted file at a file server.

27. A method according to Claim 26, wherein the step of storing the encrypted file and the file header is followed by the steps of:

retrieving the encrypted file and the associated file header from the file server;

obtaining a private key associated with the public key;

decrypting the encrypted file encryption key with the private key to provide a recovered file encryption key, a recovered integrity key and a recovered verification value;

hashing the recovered file encryption key and the recovered integrity key to provide a hash value;

comparing the hash value and the recovered verification value; and

decrypting the file with the recovered file encryption key if the comparison of the hash value and

the recovered verification value indicates that the values are equal.

28. A method according to Claim 27, further comprising the steps of:

hashing the recovered integrity key with the decrypted file to provide a recovered message authentication code;

obtaining a message authentication code from the file header; and

comparing the recovered message authentication code with the message authentication code from the file header to confirm that the decrypted file corresponds to the file which generated the message authentication code from the file header.

29. A system for controlling access to digital data in a file comprising:

means for obtaining a passphrase from a user;

means for generating a personal key based on the obtained passphrase;

means for generating a file encryption key;

means for encrypting the digital data in the file with the file encryption key to provide an encrypted file;

means for encrypting the file encryption key with the personal key to provide an encrypted file encryption key;

means for creating a file header containing the encrypted file encryption key; and

means for associating the file header with the encrypted file.

30. A system according to Claim 29, further comprising means for storing the encrypted file at a file server.

31. A system according to Claim 30, wherein the passphrase comprises a current passphrase, the system further comprising:

means for obtaining the file header associated with the encrypted file stored at the file server;

means for generating the personal key from the current passphrase associated with the file;

means for decrypting the encrypted file encryption key with the personal key to provide a recovered file encryption key;

means for generating a new personal key based on a new passphrase;

means for encrypting the file encryption key with the new personal key to provide a new encrypted file encryption key;

means for creating a new file header containing the new encrypted file encryption key; and

means for associating the new file header with the encrypted file stored at the file server.

32. A system according to Claim 31, further comprising means for storing the new file header associated with the encrypted file at the file server.

33. A system according to Claim 32, wherein a plurality of files have corresponding associated file headers containing encrypted file encryption keys encrypted with a corresponding plurality of personal keys based on the passphrase, and wherein the means for obtaining the file header associated with the encrypted file comprises means for retrieving the plurality of

file headers associated with the encrypted files from the file server;

wherein the means for generating the personal key from the current passphrase associated with the file comprises means for generating the plurality of personal keys from the current passphrase associated with the plurality of files;

wherein the means for decrypting the encrypted file encryption key with the personal key to provide a recovered file encryption key comprises means for decrypting the plurality of encrypted file encryption keys with corresponding ones of the plurality of personal keys to provide a corresponding plurality of file encryption keys;

wherein the means for generating a new personal key based on the new passphrase comprises means for generating a plurality of new personal keys based on the new passphrase;

wherein the means for encrypting the file encryption key with the new personal key to provide a new encrypted file encryption key comprises means for encrypting the plurality of file encryption keys with corresponding ones of the plurality of new personal keys to provide a plurality of new encrypted file encryption keys;

wherein the means for creating a new file header containing the new encrypted file encryption key comprises means for creating a plurality of new file headers containing the new encrypted file encryption keys; and

wherein the means for storing the new file header associated with the file at the file server comprises means for storing the plurality of new file headers associated with the plurality of files at the file server.

34. A system according to Claim 33, wherein the plurality of files comprise all files stored at the file server associated with a user and having a file header with an encrypted file encryption key encrypted with a personal key derived from the current passphrase.

35. A system according to Claim 30, further comprising:

means for obtaining a passphrase to be utilized in decrypting the file;

means for retrieving the encrypted file and the associated file header;

means for generating the personal key from the passphrase to be utilized in decrypting the file;

means for decrypting the encrypted file encryption key with the personal key to provide a recovered file encryption key; and

means for decrypting the file with the recovered file encryption key.

36. A system according to Claim 29, further comprising:

means for obtaining a user identification associated with an owner of the file;

means for obtaining a file identification associated with the file; and

wherein the means for generating a personal key based on the obtained passphrase comprises means for hashing the user identification, the passphrase and the file identification to provide the personal key.

37. A system according to Claim 36, further comprising means for storing the file and the associated file header at a file server.

38. A system according to Claim 37, wherein the means for storing the file and the associated file header at a file server comprises means for selectively storing the file and the file header based on a type of store requested by the user and an evaluation of whether an existing file and file header having the user identification and file identification are stored at the file server.

39. A system according to Claim 29, further comprising:

means for generating an integrity key;

means for generating a message authentication code based on digital data of the file utilizing the integrity key;

wherein the means for encrypting the file encryption key with the personal key to provide an encrypted file encryption key comprises means for encrypting the file encryption key and the integrity key with the personal key to provide encrypted file encryption keys; and

wherein the means for creating a file header containing the encrypted file encryption key comprises means for creating a file header containing the encrypted file encryption keys and the message authentication code.

40. A system according to Claim 39, further comprising means for storing the encrypted file and the file header associated with the encrypted file at a file server.

41. A system according to Claim 40, further comprising:

means for obtaining a passphrase to be utilized in decrypting the file;

means for retrieving the encrypted file and the associated file header from the file server;

means for generating the personal key from the passphrase to be utilized in decrypting the file;

means for decrypting the encrypted file encryption keys with the personal key to provide a recovered file encryption key and a recovered integrity key;

means for decrypting the file with the recovered file encryption key;

means for hashing the recovered integrity key with the decrypted file to provide a recovered message authentication code;

means for obtaining the message authentication code from the file header; and

means for comparing the recovered message authentication code with the message authentication code from the file header to confirm that the decrypted file corresponds to the file which generated the message authentication code from the file header.

42. A system according to Claim 39, further comprising means for hashing the file encryption key with the integrity key to provide a verification value; and

wherein the means for encrypting the file encryption key and the integrity key with the personal key to provide encrypted file encryption keys comprises means for encrypting the file encryption key, the integrity key and the verification value with the

personal key to provide the encrypted file encryption keys.

43. A system according to Claim 42, further comprising means for storing the encrypted file and the file header associated with the encrypted file at a file server.

44. A system according to Claim 43, further comprising:

means for obtaining a passphrase to be utilized in decrypting the file;

means for retrieving the encrypted file and the associated file header from the file server;

means for generating the personal key from the passphrase to be utilized in decrypting the file;

means for decrypting the encrypted file encryption key with the personal key to provide a recovered file encryption key, a recovered integrity key and a recovered verification value;

means for hashing the recovered file encryption key and the recovered integrity key to provide a hash value;

means for comparing the hash value and the recovered verification value; and

means for decrypting the file with the recovered file encryption key if the comparison of the hash value and the recovered verification value indicates that the values are equal.

45. A system according to Claim 44, further comprising:

means for hashing the recovered integrity key with the decrypted file to provide a recovered message authentication code;

means for obtaining the message authentication code from the file header; and

means for comparing the recovered message authentication code with the message authentication code from the file header to confirm that the decrypted file corresponds to the file which generated the message authentication code from the file header.

46. A system according to Claim 29, further comprising:

means for determining if a party other than an owner of the file is to have access to the file;

means for obtaining a public key associated with the party other than the owner of the file if the party other than the owner of the file is to have access to the file;

means for encrypting the file encryption key with the public key of the party other than the owner of the file to provide a public key encrypted file encryption key if the party other than the owner of the file is to have access to the file; and

means for incorporating the public key encrypted file encryption key in the header associated with the file if the party other than the owner of the file is to have access to the file.

47. A system according to Claim 46, further comprising means for storing the file header and the file at a file server.

48. A system according to Claim 47, further comprising:

means for retrieving the file and the file header from the file server;

means for obtaining a private key associated with the public key;

means for decrypting the public key encrypted file encryption key with the private key to provide the file encryption key; and

means for decrypting the file with the file encryption key.

49. A system according to Claim 46, further comprising:

means for generating an integrity key;

means for generating a message authentication code based on digital data of the file utilizing the integrity key;

wherein the means for encrypting the file encryption key with the personal key to provide an encrypted file encryption key comprises the step of encrypting the file encryption key and the integrity key with the personal key to provide encrypted file encryption keys;

wherein the means for creating a file header containing the encrypted file encryption key comprises means for creating a file header containing the encrypted file encryption keys and the message authentication code;

wherein the means for encrypting the file encryption key with the public key of the party other than the owner of the file to provide a public key encrypted file encryption key if the party other than the owner of the file is to have access to the file comprises means for encrypting the file encryption key and the integrity key with the public key to provide public key encrypted keys; and

wherein the means for incorporating the public key encrypted file encryption key in the file header

associated with the file if the party other than the owner of the file is to have access to the file comprises means for incorporating the public key encrypted keys in the file header.

50. A system according to Claim 49, further comprising means for storing the encrypted file and the file header associated with the encrypted file at a file server.

51. A system according to Claim 50, further comprising:

means for retrieving the encrypted file and the associated file header from the file server;

means for obtaining a private key associated with public key;

means for decrypting the public key encrypted keys with the private key to provide a recovered file encryption key and a recovered integrity key;

means for decrypting the file with the recovered file encryption key;

means for hashing the recovered integrity key with the decrypted file to provide a recovered message authentication code;

means for obtaining a message authentication code from the file header; and

means for comparing the recovered message authentication code with the message authentication code from the file header to confirm that the decrypted file corresponds to the file which generated the message authentication code from the file header.

52. A system according to Claim 50, wherein the public key comprises a current public key, the system further comprising:

means for retrieving the file header associated with the encrypted file from the file server;

means for generating the personal key from the passphrase associated with the file;

means for decrypting the encrypted file encryption key with the personal key to provide a recovered file encryption key;

means for obtaining a new public key;

means for encrypting the file encryption key with the new public key to provide a new public key encrypted file encryption key;

means for creating a new file header containing the new public key encrypted file encryption key; and

means for storing the new file header associated with the file at the file server.

53. A system according to Claim 49, further comprising means for hashing the file encryption key with the integrity key to provide a verification value; and

wherein the means for encrypting the file encryption key and the integrity key with the public key to provide public key encrypted keys comprises means for encrypting the file encryption key, the integrity key and the verification value with the public key to provide the public key encrypted keys.

54. A system according to Claim 53, further comprising means for storing the encrypted file and the file header associated with the encrypted file at a file server.

55. A system according to Claim 54, further comprising:

means for retrieving the encrypted file and the associated file header from the file server;

means for obtaining a private key associated with the public key;

means for decrypting the encrypted file encryption key with the private key to provide a recovered file encryption key, a recovered integrity key and a recovered verification value;

means for hashing the recovered file encryption key and the recovered integrity key to provide a hash value;

means for comparing the hash value and the recovered verification value; and

means for decrypting the file with the recovered file encryption key if the comparison of the hash value and the recovered verification value indicates that the values are equal.

56. A system according to Claim 55, further comprising:

means for hashing the recovered integrity key with the decrypted file to provide a recovered message authentication code;

means for obtaining a message authentication code from the file header; and

means for comparing the recovered message authentication code with the message authentication code from the file header to confirm that the decrypted file corresponds to the file which generated the message authentication code from the file header.

57. A computer program product for controlling access to digital data in a file comprising:

a computer readable storage medium having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code which obtains a passphrase from a user;

computer readable program code which generates a personal key based on the obtained passphrase;

computer readable program code which generates a file encryption key;

computer readable program code which encrypts the digital data in the file with the file encryption key to provide an encrypted file;

computer readable program code which encrypts the file encryption key with the personal key to provide an encrypted file encryption key;

computer readable program code which creates a file header containing the encrypted file encryption key; and

computer readable program code which associates the file header with the encrypted file.

58. A computer program product according to Claim 57, further comprising computer readable program code which stores the encrypted file at a file server.

59. A computer program product according to Claim 58, wherein the passphrase comprises a current passphrase, the computer program product further comprising:

computer readable program code which obtains the file header associated with the encrypted file stored at the file server;

computer readable program code which generates the personal key from the current passphrase associated with the file;

computer readable program code which decrypts the encrypted file encryption key with the personal key to provide a recovered file encryption key;

computer readable program code which generates a new personal key based on a new passphrase;

computer readable program code which encrypts the file encryption key with the new personal key to provide a new encrypted file encryption key;

computer readable program code which creates a new file header containing the new encrypted file encryption key; and

computer readable program code which associates the new file header with the encrypted file stored at the file server.

60. A computer program product according to Claim 59, further comprising computer readable program code which stores the new file header associated with the encrypted file at the file server.

61. A computer program product according to Claim 60, wherein a plurality of files have corresponding associated file headers containing encrypted file encryption keys encrypted with a corresponding plurality of personal keys based on the passphrase, and wherein the computer readable program code which obtains the file header associated with the encrypted file comprises computer readable program code which retrieves the plurality of file headers associated with the encrypted files from the file server;

wherein the computer readable program code which generates the personal key from the current passphrase associated with the file comprises computer readable program code which generates the plurality of personal

keys from the current passphrase associated with the plurality of files;

wherein the computer readable program code which decrypts the encrypted file encryption key with the personal key to provide a recovered file encryption key comprises computer readable program code which decrypts the plurality of encrypted file encryption keys with corresponding ones of the plurality of personal keys to provide a corresponding plurality of file encryption keys;

wherein the computer readable program code which generates a new personal key based on the new passphrase comprises computer readable program code which generates a plurality of new personal keys based on the new passphrase;

wherein the computer readable program code which encrypts the file encryption key with the new personal key to provide a new encrypted file encryption key comprises computer readable program code which encrypts the plurality of file encryption keys with corresponding ones of the plurality of new personal keys to provide a plurality of new encrypted file encryption keys;

wherein the computer readable program code which creates a new file header containing the new encrypted file encryption key comprises computer readable program code which creates a plurality of new file headers containing the new encrypted file encryption keys; and

wherein the computer readable program code which stores the new file header associated with the file at the file server comprises computer readable program code which stores the plurality of new file headers associated with the plurality of files at the file server.

62. A computer program product according to Claim 61, wherein the plurality of files comprise all files stored at the file server associated with a user and having a file header with an encrypted file encryption key encrypted with a personal key derived from the current passphrase.

63. A computer program product according to Claim 58, further comprising:

computer readable program code which obtains a passphrase to be utilized in decrypting the file;

computer readable program code which retrieves the encrypted file and the associated file header;

computer readable program code which generates the personal key from the passphrase to be utilized in decrypting the file;

computer readable program code which decrypts the encrypted file encryption key with the personal key to provide a recovered file encryption key; and

computer readable program code which decrypts the file with the recovered file encryption key.

64. A computer program product according to Claim 57, further comprising:

computer readable program code which obtains a user identification associated with an owner of the file;

computer readable program code which obtains a file identification associated with the file; and

wherein the computer readable program code which generates a personal key based on the obtained passphrase comprises computer readable program code which hashes the user identification, the passphrase and the file identification to provide the personal key.

65. A computer program product according to Claim 64, further comprising computer readable program code which stores the file and the associated file header at a file server.

66. A computer program product according to Claim 65, wherein the computer readable program code which stores the file and the associated file header at a file server comprises computer readable program code which selectively stores the file and the file header based on a type of store requested by the user and an evaluation of whether an existing file and file header having the user identification and file identification are stored at the file server.

67. A computer program product according to Claim 57, further comprising:

computer readable program code which generates an integrity key;

computer readable program code which generates a message authentication code based on digital data of the file utilizing the integrity key;

wherein the computer readable program code which encrypts the file encryption key with the personal key to provide an encrypted file encryption key comprises computer readable program code which encrypts the file encryption key and the integrity key with the personal key to provide encrypted file encryption keys; and

wherein the computer readable program code which creates a file header containing the encrypted file encryption key comprises computer readable program code which creates a file header containing the encrypted file encryption keys and the message authentication code.

68. A computer program product according to Claim 67, further comprising computer readable program code which stores the encrypted file and the file header associated with the encrypted file at a file server.

69. A computer program product according to Claim 68, further comprising:

computer readable program code which obtains a passphrase to be utilized in decrypting the file;

computer readable program code which retrieves the encrypted file and the associated file header from the file server;

computer readable program code which generates the personal key from the passphrase to be utilized in decrypting the file;

computer readable program code which decrypts the encrypted file encryption keys with the personal key to provide a recovered file encryption key and a recovered integrity key;

computer readable program code which decrypts the file with the recovered file encryption key;

computer readable program code which hashes the recovered integrity key with the decrypted file to provide a recovered message authentication code;

computer readable program code which obtains the message authentication code from the file header; and

computer readable program code which compares the recovered message authentication code with the message authentication code from the file header to confirm that the decrypted file corresponds to the file which generated the message authentication code from the file header.

70. A computer program product according to Claim 67, further comprising computer readable program code which hashes the file encryption key with the integrity key to provide a verification value; and

wherein the computer readable program code which encrypts the file encryption key and the integrity key with the personal key to provide encrypted file encryption keys comprises computer readable program code which encrypts the file encryption key, the integrity key and the verification value with the personal key to provide the encrypted file encryption keys.

71. A computer program product according to Claim 70, further comprising computer readable program code which stores the encrypted file and the file header associated with the encrypted file at a file server.

72. A computer program product according to Claim 71, further comprising:

computer readable program code which obtains a passphrase to be utilized in decrypting the file;

computer readable program code which retrieves the encrypted file and the associated file header from the file server;

computer readable program code which generates the personal key from the passphrase to be utilized in decrypting the file;

computer readable program code which decrypts the encrypted file encryption key with the personal key to provide a recovered file encryption key, a recovered integrity key and a recovered verification value;

computer readable program code which hashes the recovered file encryption key and the recovered integrity key to provide a hash value;

computer readable program code which compares the hash value and the recovered verification value; and

computer readable program code which decrypts the file with the recovered file encryption key if the comparison of the hash value and the recovered verification value indicates that the values are equal.

73. A computer program product according to Claim 72, further comprising:

computer readable program code which hashes the recovered integrity key with the decrypted file to provide a recovered message authentication code;

computer readable program code which obtains the message authentication code from the file header; and

computer readable program code which compares the recovered message authentication code with the message authentication code from the file header to confirm that the decrypted file corresponds to the file which generated the message authentication code from the file header.

74. A computer program product according to Claim 57, further comprising:

computer readable program code which determinesdetermining if a party other than an owner of the file is to have access to the file;

computer readable program code which obtains a public key associated with the party other than the owner of the file if the party other than the owner of the file is to have access to the file;

computer readable program code which encrypts the file encryption key with the public key of the party other than the owner of the file to provide a public key encrypted file encryption key if the party other

than the owner of the file is to have access to the file; and

computer readable program code which incorporates incorporating the public key encrypted file encryption key in the header associated with the file if the party other than the owner of the file is to have access to the file.

75. A computer program product according to Claim 74, further comprising computer readable program code which stores the file header and the file at a file server.

76. A computer program product according to Claim 75, further comprising:

computer readable program code which retrieves the file and the file header from the file server;

computer readable program code which obtains a private key associated with the public key;

computer readable program code which decrypts the public key encrypted file encryption key with the private key to provide the file encryption key; and

computer readable program code which decrypts the file with the file encryption key.

77. A computer program product according to Claim 74, further comprising:

computer readable program code which generates an integrity key;

computer readable program code which generates a message authentication code based on digital data of the file utilizing the integrity key;

wherein the computer readable program code which encrypts the file encryption key with the personal key to provide an encrypted file encryption key comprises

the step of encrypting the file encryption key and the integrity key with the personal key to provide encrypted file encryption keys;

wherein the computer readable program code which creates a file header containing the encrypted file encryption key comprises computer readable program code which creates a file header containing the encrypted file encryption keys and the message authentication code;

wherein the computer readable program code which encrypts the file encryption key with the public key of the party other than the owner of the file to provide a public key encrypted file encryption key if the party other than the owner of the file is to have access to the file comprises computer readable program code which encrypts the file encryption key and the integrity key with the public key to provide public key encrypted keys; and

wherein the computer readable program code which incorporates the public key encrypted file encryption key in the file header associated with the file if the party other than the owner of the file is to have access to the file comprises computer readable program code which incorporates the public key encrypted keys in the file header.

78. A computer program product according to Claim 77, further comprising computer readable program code which stores the encrypted file and the file header associated with the encrypted file at a file server.

79. A computer program product according to Claim 78, further comprising:

computer readable program code which retrieves the encrypted file and the associated file header from the file server;

computer readable program code which obtains a private key associated with public key;

computer readable program code which decrypts the public key encrypted keys with the private key to provide a recovered file encryption key and a recovered integrity key;

computer readable program code which decrypts the file with the recovered file encryption key;

computer readable program code which hashes the recovered integrity key with the decrypted file to provide a recovered message authentication code;

computer readable program code which obtains a message authentication code from the file header; and

computer readable program code which compares the recovered message authentication code with the message authentication code from the file header to confirm that the decrypted file corresponds to the file which generated the message authentication code from the file header.

80. A computer program product according to Claim 78, wherein the public key comprises a current public key, the computer program product further comprising:

computer readable program code which retrieves the file header associated with the encrypted file from the file server;

computer readable program code which generates the personal key from the passphrase associated with the file;

computer readable program code which decrypts the encrypted file encryption key with the personal key to provide a recovered file encryption key;

computer readable program code which obtains a new public key;

computer readable program code which encrypts the file encryption key with the new public key to provide a new public key encrypted file encryption key;

computer readable program code which creates a new file header containing the new public key encrypted file encryption key; and

computer readable program code which stores the new file header associated with the file at the file server.

81. A computer program product according to Claim 77, further comprising computer readable program code which hashes the file encryption key with the integrity key to provide a verification value; and

wherein the computer readable program code which encrypts the file encryption key and the integrity key with the public key to provide public key encrypted keys comprises computer readable program code which encrypts the file encryption key, the integrity key and the verification value with the public key to provide the public key encrypted keys.

82. A computer program product according to Claim 81, further comprising computer readable program code which stores the encrypted file and the file header associated with the encrypted file at a file server.

83. A computer program product according to Claim 82, further comprising:

computer readable program code which retrieves the encrypted file and the associated file header from the file server;

computer readable program code which obtains a private key associated with the public key;

computer readable program code which decrypts the encrypted file encryption key with the private key to provide a recovered file encryption key, a recovered integrity key and a recovered verification value;

computer readable program code which hashes the recovered file encryption key and the recovered integrity key to provide a hash value;

computer readable program code which compares the hash value and the recovered verification value; and

computer readable program code which decrypts the file with the recovered file encryption key if the comparison of the hash value and the recovered verification value indicates that the values are equal.

84. A computer program product according to Claim 83, further comprising:

computer readable program code which hashes the recovered integrity key with the decrypted file to provide a recovered message authentication code;

computer readable program code which obtains a message authentication code from the file header; and

computer readable program code which compares the recovered message authentication code with the message authentication code from the file header to confirm that the decrypted file corresponds to the file which generated the message authentication code from the file header.